**

Cloud Security Policy Template

Creating a cloud security policy is a best practice. An essential part of your cloud security strategy, this policy helps your organization properly store and protect your critical data assets. It shows who is responsible for each aspect of cyber security, details your approach to cloud services and provides written evidence of your commitment to protecting enterprise data. Moreover, a documented cloud security policy document is a re- quirement of some compliance regulations.

A cloud security policy is not a stand-alone document. You must link it to other security policies developed within your organization, such as your data security and privacy policies.

The cloud security policy template below provides a road map of recommended key sections, with descriptions and examples. Adapt it to meet your organization’s unique legal and regulatory requirements.

## Purpose

The purpose section of a cloud security policy should clearly outline the **reasons** why the organization developed and maintains the policy.

Here's a reframing of the purpose based on your point:

* **To Secure Cloud Resources:** The policy establishes a comprehensive approach to safeguarding the organization's data, applications, and infrastructure within the cloud environment.
* **To Ensure Compliance:** The policy outlines the procedures to follow to meet industry regulations and internal security standards.
* **To Promote Consistent Security Practices:** The policy defines the expected behaviors and best practices for everyone using cloud resources, fostering a culture of security awareness.
* **To Assign Clear Roles and Responsibilities:** The policy clarifies the ownership and accountability for different aspects of cloud security within the organization.

## Scope

This section of a cloud security policy defines the **scope**, which outlines **where the policy applies**. It specifies which aspects of the cloud environment are covered by the policy's guidelines and security controls. Here are some common elements you might find in a scope section:

* **Covered Cloud Services:** This section identifies the specific cloud services the policy applies to. This could include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) offerings used by the organization.
* **Protected Data:** The scope should define the types of data the policy protects within the cloud environment. This might include sensitive customer information, intellectual property, financial data, or any other data classified as requiring specific security measures.
* **Applicable Users and Groups:** The policy should specify which user groups and individuals fall under the scope of the policy. This could include all employees, contractors, or any third-party users with access to the organization's cloud resources.
* **Geographic Locations:** In some cases, the policy might be relevant only for specific geographic locations where cloud data centers are situated or where cloud resources are accessed.
* **Exclusions:** The scope section may also outline any exclusions or limitations to the policy's coverage. For example, it might specify that the policy doesn't apply to personal cloud storage used by employees.

* 1. Information Types

## Information Types Covered by this Policy

This policy applies to all cloud-based data storage, processing, and access within our organization. To ensure appropriate security measures are implemented, we will classify data based on its sensitivity and risk profile. Here are the information types covered under this policy, categorized using data classification best practices:

**Highly Confidential**

* **Financial Data:** This includes sensitive financial information such as bank account details, credit card numbers, tax records, and investment data. (**Data Classification Label:** FIN-HIGH)
* **Personal Identifiable Information (PII):** This encompasses any data that can be used to identify an individual, such as Social Security numbers, passport details, driver's licenses, and health records. (**Data Classification Label:** PII-HIGH)
* **Intellectual Property (IP):** This includes proprietary information like trade secrets, patents, copyrights, and source code. (**Data Classification Label:** IP-HIGH)

**Confidential**

* **Customer Data:** This includes customer names, contact details, purchase history, and any other information related to customer interactions. (**Data Classification Label:** CUSTOMER-CONF)
* **Employee Data:** This encompasses employee information such as salary details, performance reviews, and health insurance information. (**Data Classification Label:** EMPLOYEE-CONF)
* **Internal Business Data:** This includes sensitive internal documents, financial reports, and strategic plans. (**Data Classification Label:** INTERNAL-CONF)

**Public**

* **Marketing Materials:** This includes publicly available information such as brochures, website content, and press releases. (**Data Classification Label:** PUBLIC)
* **Non-Sensitive Training Materials:** This encompasses publicly accessible training materials that are not confidential. (**Data Classification Label:** PUBLIC)

## Ownership and Responsibilities

Here are the key roles related to cloud security actions, controls, and procedures for Initrobe:

**1. Cloud Security Administrator (CSA):**

* **Description:** This role, potentially filled by an internal hire or outsourced to your MSSP, oversees the implementation and management of security controls for Initrobe's cloud environment. They will be responsible for tasks like:
  + Configuring and maintaining security settings in cloud platforms (AWS, Heroku).
  + Enforcing access controls and identity management.
  + Implementing data encryption at rest and in transit.
  + Monitoring cloud security logs for suspicious activity.
  + Responding to security incidents.
  + Maintaining security policies and procedures.

**2. Data Owner:**

* **Description:** This role can be assigned to specific individuals or departments depending on the data type. They are accountable for understanding the sensitivity of the data they manage and ensuring its proper security. Responsibilities include:
  + Classifying data based on sensitivity (public, confidential, etc.).
  + Determining appropriate data access controls.
  + Implementing data loss prevention (DLP) measures.
  + Participating in security awareness training related to data handling.

**3. Users:**

* **Description:** This includes all Initrobe employees and contractors who access cloud resources. They play a crucial role in maintaining good security hygiene by following security policies and procedures. Responsibilities include:
  + Using strong and unique passwords with MFA enabled.
  + Reporting suspicious activity or security incidents.
  + Avoiding sharing login credentials or access with others.
  + Keeping software on their devices updated.
  + Completing security awareness training.

**4. Cloud Provider (AWS, Heroku):**

* **Description:** While Initrobe is responsible for securing its data and workloads within the cloud environment, the cloud provider also plays a role. They are responsible for:
  + Securing the underlying infrastructure of their cloud platform.
  + Providing security features and tools for their customers (Initrobe).
  + Maintaining compliance with relevant security standards.

**5. IT Management/MSSP:**

* **Description:** In the absence of a dedicated IT department, your MSSP can potentially take on some or all of the Cloud Security Administrator responsibilities. This would include configuration, management, and monitoring of security controls within the cloud environment.

**6. Management (CTO, CEO):**

* **Description:** Senior management ultimately makes significant decisions regarding security investments and resource allocation. They are responsible for:
  + Approving security policies and procedures.
  + Allocating budget for security tools and training.
  + Overseeing the overall security posture of the organization.
  + Providing leadership and direction for the security program.

**7. Security Architect:**

* **Description:** This role can be internal or outsourced and is responsible for designing and implementing a secure cloud architecture for Initrobe. Responsibilities include:
  + Selecting secure cloud services and configurations.
  + Designing network segmentation and access controls.
  + Integrating security solutions with cloud platforms.

While not an exhaustive list, these roles and their associated responsibilities provide a good starting point for establishing a strong cloud security posture for Initrobe. As your MSSP, you can work with Initrobe to clearly define these roles and ensure everyone understands their part in maintaining a secure cloud environment.

## Secure Usage of Cloud Computing Services

Initrobe relies heavily on cloud services to conduct business. To ensure the security and privacy of our data, as well as the continued smooth operation of our services, this Acceptable Use Policy (AUP) outlines the expectations for all employees, contractors, and any other authorized users who access Initrobe data or systems through cloud services.

**1. Authorized Use**

* Cloud services are for authorized business purposes only. Personal use is strictly prohibited.
* Users are only authorized to access cloud resources and data assigned to them based on their job function and department.
* Sharing login credentials or access to cloud resources with unauthorized individuals is strictly forbidden.

**2. Data Security**

* Users are responsible for safeguarding all company data accessed or stored in the cloud. This includes:
  + Following strong password practices (complex passwords, avoid reuse) and enabling Multi-Factor Authentication (MFA) wherever available.
  + Downloading and storing sensitive data only when absolutely necessary and following company procedures for data encryption at rest and in transit.
  + Reporting any suspected data breaches or unauthorized access attempts immediately.

**3. Security Awareness**

* All Initrobe personnel (employees and contractors) will be required to complete security awareness training to understand cybersecurity best practices and their role in protecting company data.

**4. Device Management**

* Company-issued devices must be configured according to Initrobe security standards, including:
  + Full disk encryption
  + Automatic screen lock after a period of inactivity
  + Up-to-date antivirus and anti-malware software with active scanning
  + Automatic operating system updates enabled
  + Use of a reputable password manager application

**5. Third-Party Applications and Services**

* Users must avoid downloading or using unauthorized cloud applications or services on company devices.
* Any need for additional cloud-based tools must be pre-approved by the IT department (MSSP in this case) to ensure compatibility with security protocols.

**6. Consequences of Violation**

Violations of this AUP may result in disciplinary action, up to and including termination of employment or contractor agreements.

**7. Review and Updates**

This AUP will be reviewed and updated periodically to reflect changes in technology, security threats, and company practices.

* 1. Inventory

Non Apliccable

### Approved Services

The organization has a central headquarters and several offices located throughout the USA. Some employees access services remotely from mobile devices. Each department—such as human resources, sales, and project management—uses one or more cloud services. All departments must maintain a list of authorized cloud providers and services that are aligned with the overall cloud security policy.

The list of approved services includes:

 Hardware layer: Non-applicable

 Infrastructure layer: GCP

 Platform layer: Google APP engine

 Application layer: Business Application

### Unauthorized Services

## Non-Permitted Cloud-Based Services at Initrobe

To maintain a strong security posture and ensure compliance with regulations, the following cloud-based services are not permitted for use at Initrobe:

* **Unauthorized Cloud Storage:** Downloading or using personal cloud storage services (e.g., Dropbox, Google Drive for personal use) to store or share Initrobe data is strictly prohibited.
* **Unvetted Cloud Applications:** Employees and contractors cannot install or use cloud-based applications that haven't been reviewed and approved by the IT department (MSSP). This ensures compatibility with Initrobe's security protocols and minimizes the risk of introducing vulnerabilities.
* **Shadow IT:** The use of any unauthorized cloud service outside of the approved tools and platforms is strictly forbidden. This includes services used for file sharing, communication, project management, or any other business function that haven't been vetted by IT.

**Exceptions:**

* In limited circumstances and with prior written approval from the IT department, exceptions to this policy may be granted for specific business needs. However, such exceptions will require a thorough security review to ensure the chosen service meets Initrobe's security standards.

## Risk Assessment

Initrobe's cloud security policy and risk assessment policy will work hand-in-hand to proactively identify and mitigate security threats within our cloud environment.

**Risk Assessments:**

* **Scope:** Regular risk assessments will be conducted to evaluate the security posture of Initrobe's cloud infrastructure, applications, and data. This assessment will encompass:
  + Cloud service providers (AWS, Heroku, Google Workspace) and their security controls.
  + Third-party cloud-based applications and services used by Initrobe personnel.
  + Internal security controls, including access management, data encryption, and incident response procedures.
  + User behavior and adherence to the Acceptable Use Policy (AUP) for cloud services.
* **Schedule:** Formal risk assessments will be conducted:
  + **Annually:** A comprehensive assessment will be performed to identify any new or emerging threats and ensure alignment with evolving industry security standards.
  + **Quarterly:** Focused assessments will target specific areas of the cloud environment based on ongoing monitoring and threat intelligence.
  + **Incident Driven:** Additional risk assessments will be triggered in response to security incidents or potential vulnerabilities discovered through monitoring or user reports.

**Integration with Cloud Security Policy:**

The findings from the risk assessments will directly inform updates to the Cloud Security Policy. Identified risks will be categorized based on likelihood and severity, and corresponding mitigation strategies will be implemented. The Cloud Security Policy will be reviewed and updated at least annually, or more frequently to reflect changes in the risk landscape or security best practices.

**Benefits of Integration:**

By integrating risk assessments with the cloud security policy, Initrobe can achieve:

* **Proactive Threat Management:** Regular assessments help identify and address potential security issues before they can be exploited.
* **Resource Optimization:** Focuses security efforts on the most critical areas based on identified risks.
* **Compliance Assurance:** Aligns security practices with relevant industry regulations and standards.
* **Continuous Improvement:** Provides a feedback loop for refining security controls and policies for a more secure cloud environment.

## Security Controls

At the time of cloud service implementation and quarterly after that, the Coud Security Administrator shall review each service-lever agreement, as well as request and analyze the cloud provider’s security audits

* 1. Technical Security Controls Requirements

This section outlines the various security controls implemented at Initrobe to safeguard our cloud environment, encompassing both internal controls and those offered by our cloud service providers (CSPs).

**1. Identity and Access Management (IAM):**

* **Technical Controls:**
  + **Multi-Factor Authentication (MFA):** Enforced for all logins to critical systems and cloud platforms (Heroku, AWS, GitHub, Initron platform access).
  + **Strong Password Policies:** Enforced minimum password length, complexity requirements, and regular password rotation for Google Workspace and other applicable platforms.
  + **Least Privilege Access:** Granting users only the minimum level of access required to perform their jobs.
  + **Access Reviews:** Regularly reviewing and revoking access privileges for inactive users or those whose roles have changed.
* **CSP Controls:** We leverage the granular access control features offered by our CSPs (AWS IAM, Heroku Access Control) to manage user permissions within their platforms.

**2. Data Security:**

* **Technical Controls:**
  + **Data Encryption:** Data at rest and in transit will be encrypted using industry-standard algorithms. This includes encrypting hard drives on company-issued laptops and encrypting data stored in cloud storage services.
  + **Data Classification:** Data will be classified based on sensitivity (confidential, public, etc.) to determine appropriate security controls.
  + **Data Loss Prevention (DLP):** Implementing DLP solutions to prevent unauthorized data exfiltration through cloud services.
* **CSP Controls:** Utilizing data encryption features offered by our CSPs (e.g., AWS KMS, Heroku Shield) to further protect data confidentiality.

**3. Network Security:**

* **Technical Controls:**
  + **Firewalls:** Implementing firewalls to restrict unauthorized access to Initrobe's cloud resources.
  + **Network Segmentation:** Segmenting the cloud environment to isolate critical systems and data from less sensitive resources.
  + **Secure Configuration of Cloud Resources:** Following security best practices for configuring cloud services like AWS and Heroku to minimize vulnerabilities.
* **CSP Controls:** Relying on the network security controls implemented by our CSPs to protect their underlying infrastructure.

**4. Mobile Security (if applicable):**

* **Technical Controls:**
  + **Mobile Device Management (MDM):** Implementing MDM software to manage and secure access to Initrobe resources from mobile devices (if/when company-issued phones are introduced). This may include enforcing strong passwords, remote wipe capabilities, and application whitelisting.
  + **Mobile Security Awareness Training:** Educating users on secure mobile practices to minimize risks associated with accessing company data on personal devices.

### Mobile Security Requirements **Mobile Security (if applicable):**

* **Technical Controls:**
  + **Mobile Device Management (MDM):** Implementing MDM software to manage and secure access to Initrobe resources from mobile devices (if/when company-issued phones are introduced). This may include enforcing strong passwords, remote wipe capabilities, and application whitelisting.
  + **Mobile Security Awareness Training:** Educating users on secure mobile practices to minimize risks associated with accessing company data on personal devices.

### Physical Security Requirements

Non applicable

### Security Controls Assurance

**Security Controls Assurance Practices:**

* **Regular Security Reviews:** Conducting periodic reviews of security controls to ensure effectiveness and identify areas for improvement. This may include penetration testing and vulnerability assessments.
* **Vendor Risk Management:** Assessing the security posture of our cloud service providers through audits or questionnaires.
* **Security Incident and Event Management (SIEM):** Implementing a SIEM solution to centralize log collection and analysis from various cloud resources for timely detection and response to security incidents.

## Security Incident Recovery

Initrobe's cloud security policy includes a clearly defined incident response plan to ensure a swift and effective response to security incidents impacting our cloud environment. This section outlines the process for determining the areas for assessment and prioritizes cloud service and data recovery efforts.

**1. Incident Identification and Reporting:**

* Any suspected security incidents must be reported immediately to the designated security contact (SOC team or MSSP). This includes suspicious activity logs, phishing attempts, or data breaches.

**2. Incident Response Team (IRT) Activation:**

* Upon notification of a potential incident, the IRT will be activated. This team will include representatives from IT (MSSP), Security, Engineering, and potentially Legal and HR depending on the nature of the incident.

**3. Incident Assessment and Scoping:**

* The IRT will conduct a thorough investigation to determine the nature and scope of the incident. This may involve:
  + Identifying the impacted systems and data.
  + Determining the root cause of the incident.
  + Assessing the potential impact on the business, including data loss, disruption of operations, and reputational damage.

**4. Prioritization and Containment:**

* Based on the assessment, the IRT will prioritize containment actions to minimize further damage. This may include:
  + Isolating compromised systems to prevent lateral movement of the attacker.
  + Revoking access privileges of compromised accounts.
  + Disabling compromised cloud resources.

**5. Eradication and Recovery:**

* Once the incident is contained, the IRT will focus on eradication by eliminating the root cause of the incident and preventing its recurrence. This may involve:
  + Patching vulnerabilities exploited in the attack.
  + Removing malware or unauthorized software.
  + Restoring affected systems and data from backups.

**6. Post-Incident Review and Reporting:**

* After the incident is resolved, the IRT will conduct a comprehensive review to identify lessons learned and improve future incident response capabilities.
* A detailed report will be documented outlining the incident details, response actions taken, and preventative measures implemented to minimize the risk of similar incidents in the future.

**Prioritization of Cloud Service and Data Recovery:**

* During the incident response, the IRT will prioritize recovery efforts based on criticality. This may involve:
  + **Focus on restoring critical business functions first:** This could include regaining access to essential applications or data required for core operations.
  + **Prioritize recovery of sensitive data:** Data classified as highly confidential or regulated will be prioritized for restoration to minimize potential legal or compliance risks.
  + **Phased recovery of remaining systems and data:** Once critical functions and sensitive data are recovered, the IRT will focus on restoring remaining systems and data based on business needs and impact.

## Awareness-Raising

Initrobe will implement a comprehensive security awareness training program to educate employees and contractors on cybersecurity best practices and their role in protecting company data.

**Training Frequency:**

* Security awareness training will be conducted for all employees and contractors on a regular basis. The recommended frequency is **quarterly (every 3 months)** to reinforce key concepts and address evolving threats.
* New employee onboarding will include mandatory security awareness training covering company policies, password hygiene, phishing awareness, and reporting procedures.

**Training Audience:**

* All Initrobe employees, regardless of role or department, are required to complete security awareness training.
* Contractors who have access to Initrobe data or systems will also be required to complete the training.

**Training Responsibility:**

* The MSSP, in collaboration with Initrobe's IT department (or a designated security champion within Initrobe), will be responsible for developing and delivering security awareness training content.
* The training can be delivered through a combination of methods, including:
  + Online modules
  + Live webinars
  + Interactive simulations (phishing tests)
  + In-person training sessions (if feasible)

**Benefits:**

* Regularly educating employees and contractors on cybersecurity helps to:
  + Raise awareness of potential security threats.
  + Improve user behavior and decision-making regarding data security.
  + Reduce the risk of falling victim to phishing attacks and social engineering scams.
  + Foster a culture of security within the organization.

## Enforcement

Initrobe is committed to maintaining a secure cloud environment. To achieve this, compliance with this Cloud Security Policy is mandatory for all employees, contractors, and anyone authorized to access Initrobe data or systems through cloud services. Violations of this policy may result in disciplinary action, up to and including termination of employment or contractor agreements.

**Policy Enforcement:**

* The IT department (MSSP) will be responsible for monitoring and enforcing adherence to this policy. This may involve:
  + Conducting periodic security audits and reviews.
  + Monitoring user activity within the cloud environment.
  + Investigating potential security incidents and policy violations.

**Consequences of Violations:**

The severity of disciplinary action taken for policy violations will be determined based on the nature and intent of the violation, as well as any potential harm caused. Consequences may include:

* **Verbal or written warnings:** For minor, first-time offenses.
* **Mandatory retraining:** Employees or contractors who violate the policy due to lack of knowledge will be required to undergo additional security awareness training.
* **Suspension or termination of access:** Access to cloud resources or systems may be suspended or terminated for repeated or serious violations.
* **Disciplinary action up to termination:** For egregious violations that compromise sensitive data or put the organization at significant risk, disciplinary action up to termination of employment or contractor agreements may be taken.

**Reporting Violations:**

Employees and contractors are encouraged to report any suspected policy violations or security incidents to the designated security contact (SOC team or MSSP) immediately. Reports can be made anonymously if desired.

## Related Documents

This section lists all documents related to the cloud security policy and procedures. Example:

## Revision History

Maintain a history of the policy document, with entries for the original implementation and each time it is changed. Example:

| **Version** | **Revision Date** | **Author** | **Description** |
| --- | --- | --- | --- |
| 1.0 | 02/01/2020 | Elaine Parker, Cloud Security Admin | Initial Version |
| 1.1 | 06/01/2020 | Elaine Parker, Cloud Security Admin | Updates to training frequency |

**

# Conclusion

Using this cloud computing security policy example, you can develop a solid cloud security policy for your organization that enables you to protect sensitive data. Make the policy robust and feasible, and ensure it is accessible, concise and easy to understand at every level of the company.



**

**Ensure the Security of Your Microsoft 365 Environment with Netwrix Solutions**

Accurately identify sensitive information in the cloud and automatically reduce its exposure

Harden security by seeing through the tangled permissions structure of cloud-based systems and spotting broken inheritance

Know right away about changes to configuration and

permissions that could compromise security

Detect even the most clever threat actors with advanced user behavior analytics

Troubleshoot incidents quickly with Google-like search of audit data

[**Download Free 20-Day Trial**](https://www.netwrix.com/sharepoint_auditing.html?utm_source=content&utm_medium=guide&utm_campaign=cloud-security-policy)



# About Netwrix

Netwrix is a software company that enables information security and governance professionals to reclaim control over sensitive, regulated and business-critical data, regardless of where it resides. Over 10,000 organi- zations worldwide rely on Netwrix solutions to secure sensitive data, realize the full business value of enterprise content, pass compliance audits with less effort and expense, and increase the productivity of IT teams and knowledge workers.

Founded in 2006, Netwrix has earned more than 150 industry awards and been named to both the Inc. 5000 and Deloitte Technology Fast 500 lists of the fastest growing companies in the U.S.

For more infroamtion, visit [www.netwrix.com](https://www.netwrix.com/?utm_source=content&utm_medium=guide&utm_campaign=cloud-security-policy).

# Next Steps

**Free trial** — Set up Netwrix in your own test environment: [netwrix.com/freetrial](https://www.netwrix.com/products.html?utm_source=content&utm_medium=guide&utm_campaign=cloud-security-policy)

**In-Browser Demo** — Take an interactive product demo in your browser: [netwrix.com/browser\_demo](https://www.netwrix.com/browser_demo.html?utm_source=content&utm_medium=guide&utm_campaign=cloud-security-policy)

**Live Demo** — Take a product tour with a Netwrix expert: [netwrix.com/livedemo](https://www.netwrix.com/one-to-one.html?utm_source=content&utm_medium=guide&utm_campaign=cloud-security-policy)

**Request Quote** — Receive pricing information: [netwrix.com/buy](https://www.netwrix.com/how_to_buy.html?utm_source=content&utm_medium=guide&utm_campaign=cloud-security-policy)

| **CORPORATE HEADQUARTER: PHONES:** | | **OTHER LOCATIONS:** | |
| --- | --- | --- | --- |
| 300 Spectrum Center Drive | 1-949-407-5125 | Spain: | +34 911 982608 |
| Suite 200 Irvine, CA 92618 | Toll-free (USA): 888-638-9749 | Netherlands: | +31 858 887 804 |
|  |  | Sweden: | +46 8 525 03487 |

**SOCIAL:**

| Dublin, OH 43017 | 1-201-490-8840 | France: | +33 9 75 18 11 19 |
| --- | --- | --- | --- |
|  |  | Germany: | +49 711 899 89 187 |
| 5 New Street Square | +44 (0) 203 588 3023 | Hong Kong: | +852 5808 1306 |
| London EC4A 3TW |  | Italy: | +39 02 947 53539 |

565 Metro Place S, Suite 400

Switzerland:

+41 43 508 3472

[netwrix.com/social](https://www.netwrix.com/social_communities.html?utm_source=content&utm_medium=guide&utm_campaign=cloud-security-policy)

**

